# 日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

| | |
|---|---|
| 出願年月日<br>Date of Application: | 1999年 9月 6日 |
| 出願番号<br>Application Number: | 平成11年特許願第251660号 |
| 出願人<br>Applicant (s): | セイコーエプソン株式会社 |

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 8月25日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特2000-3068859

【書類名】　特許願

【整理番号】　SE990305

【提出日】　平成11年 9月 6日

【あて先】　特許庁長官　殿

【国際特許分類】　H04N　5/225

【発明の名称】　デジタルカメラおよび画像改竄検出システム

【請求項の数】　6

【発明者】

【住所又は居所】　長野県諏訪市大和三丁目３番５号　セイコーエプソン株式会社内

【氏名】　中島　靖雅

【発明者】

【住所又は居所】　長野県諏訪市大和三丁目３番５号　セイコーエプソン株式会社内

【氏名】　最上　和人

【特許出願人】

【識別番号】　000002369

【氏名又は名称】　セイコーエプソン株式会社

【代理人】

【識別番号】　100093779

【弁理士】

【氏名又は名称】　服部　雅紀

【手数料の表示】

【予納台帳番号】　007744

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1



出証特２０００－３０６８８５９

【包括委任状番号】　9901019

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　デジタルカメラおよび画像改竄検出システム

【特許請求の範囲】

【請求項１】　撮影対象からの光を画像データに変換する撮像部と、

前記画像データから第１の特徴データを生成する手段と、

公開鍵によって復号可能に暗号化するための秘密鍵を記録する秘密鍵記録部と

前記特徴データを前記秘密鍵により暗号化する手段と、

前記画像データに暗号化した特徴データを埋め込む手段と、

前記第１の特徴データを埋め込んだ画像データを記録する記録媒体と、

前記秘密鍵を外部記録媒体から転送する手段と、

を備えることを特徴とするデジタルカメラ。

【請求項２】　撮影対象からの光を画像データに変換する撮像部と、

前記画像データから第１の特徴データを生成する手段と、

公開鍵によって復号可能に暗号化するための秘密鍵を記録する秘密鍵記録部と

前記特徴データを前記秘密鍵により暗号化する手段と、

前記画像データに暗号化した特徴データを埋め込む手段と、

前記第１の特徴データを埋め込んだ画像データを記録する記録媒体とを備え、

前記秘密鍵は、前記秘密鍵記録部に隠し属性で記録されることを特徴とするデジタルカメラ。

【請求項３】　撮影対象からの光を画像データに変換するデジタルカメラに機能を付加する方法であって、

公開鍵によって復号可能に暗号化するための秘密鍵のデータ量を、複数の大きさから選択する手順と、

前記秘密鍵を外部記録媒体から前記デジタルカメラの秘密鍵記録部に記録する手順と、

前記秘密鍵を用いてデータを暗号化するプログラムを前記デジタルカメラに導入する手順と、

を含むことを特徴とするデジタルカメラの機能付加方法。

【請求項４】　前記秘密鍵は、隠し属性で記録されていることを特徴とする請求項３記載のデジタルカメラの機能付加方法。

【請求項５】　請求項１または２のいずれかに記載のデジタルカメラを用いた画像改竄検出システムであって、

前記画像データを入力する手段と、

前記画像データから暗号化された第１の特徴データを取り除く手段と、

前記暗号化された第１の特徴データを復号化する手段と、

前記暗号化された第１の特徴データを取り除いた画像データから第２の特徴データを生成する手段と、

前記復号化された第１の特徴データと前記第２の特徴データとを比較する手段と、

を備えることを特徴とする画像改竄検出システム。

【請求項６】　複数の前記秘密鍵に対応する複数の公開鍵を記録する手段を備えることを特徴とする請求項５記載の画像改竄検出システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、撮影した画像をデジタルデータとして記録するデジタルカメラ、デジタルカメラに機能を付加する方法、およびデジタルカメラにより記録された画像データの改竄を検出するシステムに関するものである。

【０００２】

【従来の技術】

従来より、写真を撮影するときには、レンズから取り込まれた光がフィルムの上に照射され、化学反応が起きることで画像が記録されるカメラが用いられている。上記のカメラでは、フィルムを現像し、印画紙に焼き付けることにより写真をプリントすることができる。上記の化学反応として一般に塩化銀の反応が利用されるため、このようなカメラによって撮影された写真を銀塩写真という。

【０００３】

一方、近年ではＣＣＤ等の光センサにより光を電気信号に変換し、それをデジタル信号に変換してから、フラッシュメモリ等の記録媒体に記録するデジタルカメラが普及している。デジタルカメラを用いると、パーソナルコンピュータ等の処理装置を用いて画像の保存や様々な加工を個人で手軽に行えるほか、プリンタで出力することによりフィルムの現像をすることなしに写真を印刷することができる。プリンタの印刷品質の向上により、銀塩写真とほとんど区別がつかないほど品質の高い写真も印刷できるようになってきている。

【０００４】

【発明が解決しようとする課題】

しかしながら、損害保険等の証明写真に用いようとする場合など、重要な証拠写真にデジタルカメラで撮影した写真を用いると、デジタルカメラで撮影された画像はパーソナルコンピュータ等により容易に加工が可能であり、銀塩写真と比較して加工の跡を残さずに加工することが容易であるため、不正に改竄された写真が用いられていても判別することが困難であり、悪用される恐れがあるという問題がある。

【０００５】

したがって、本発明の目的は撮影時の画像データから改竄されたか否かを検出することのできる画像データを出力するデジタルカメラおよびそれを用いた画像改竄検出システムを提供することにある。

【０００６】

【課題を解決するための手段】

本発明の請求項１記載のデジタルカメラによれば、画像データから第１の特徴データを生成する手段と、公開鍵によって復号可能に暗号化するための秘密鍵を記録する秘密鍵記録部と、特徴データを秘密鍵により暗号化する手段と、画像データに暗号化した特徴データを埋め込む手段と、第１の特徴データを埋め込んだ画像データを記録する記録媒体と、秘密鍵を外部記録媒体から転送する手段とを備える。したがって、デジタルカメラによる撮影時に記録媒体に記録された画像データが、その後に１ビットでも変更された場合には、画像データと第１の特徴データとが不整合となる、あるいは特徴データが破壊されるため、撮影後に画像

データが改竄されたと判断することができる。また、万一秘密鍵が他人に知られてしまったような場合であっても、別の秘密鍵を外部記録媒体から転送して書き換えることにより安全に使用することができる。

【０００７】

本発明の請求項２記載のデジタルカメラによれば、画像データから第１の特徴データを生成する手段と、公開鍵によって復号可能に暗号化するための秘密鍵を記録する秘密鍵記録部と、特徴データを秘密鍵により暗号化する手段と、画像データに暗号化した特徴データを埋め込む手段と、第１の特徴データを埋め込んだ画像データを記録する記録媒体とを備え、秘密鍵は秘密鍵記録部に隠し属性で記録される。そのため、秘密鍵の内容が容易に読み出されることがない。

【０００８】

本発明の請求項３記載のデジタルカメラに機能を付加する方法によれば、公開鍵によって復号可能に暗号化するための秘密鍵のデータ量を、複数の大きさから選択する手順と、秘密鍵を前記デジタルカメラの秘密鍵記録部に記録する手順と、秘密鍵を用いてデータを暗号化する手段を付加する手順とを含む。これにより、簡易な暗号化でよい場合と、特に信頼性が必要な場合とで暗号化のレベルを使い分けることができる。

【０００９】

本発明の請求項５に記載の画像改竄検出システムによれば、画像データを入力する手段と、画像データから暗号化された第１の特徴データを取り除く手段と、暗号化された第１の特徴データを復号化する手段と、暗号化された第１の特徴データを取り除いた画像データから第２の特徴データを生成する手段と、復号化された第１の特徴データと第２の特徴データとを比較する手段とを備える。そのため、第１の特徴データと第２の特徴データとが一致していれば、入力された画像データがデジタルカメラによって記録された後に変更されていないことを検出することができる。

【００１０】

本発明の請求項６記載の画像改竄検出システムによれば、複数の秘密鍵に対応する複数の公開鍵を記録する手段を備える。そのため、特徴データの生成方法、

暗号化方法、画像データへの埋め込み方などのアルゴリズムを知る者が、自分で公開鍵と秘密鍵の組み合わせを作成し、本発明と同様の処理を行った場合でも、あらかじめ用意された公開鍵と異なるものであれば、その画像データは改竄された可能性があると判断することができる。なお、画像改竄検出システムに記録される複数の公開鍵が知られたとしても、公開鍵から秘密鍵を算出することはほぼ不可能であるため、秘密鍵が他人に知られる恐れはない。

【００１１】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。

図２は本発明の実施例のデジタルカメラ１を説明するためのブロック図である。制御部１１、集光レンズ１２、光センサとしてのＣＣＤ（Charge Coupled Device）１３、Ａ／Ｄ変換部１４、ＲＡＭ（Random Access Memory）１５、画像データを記録する画像記録媒体としてのフラッシュメモリ１６、フラッシュメモリ１６の内容を外部のパーソナルコンピュータ２０と入出力するためのインターフェイス１７、画像を表示可能な液晶表示部（ＬＣＤ）１９などから構成される。制御部１１はＣＰＵと、デジタルカメラ１の様々な制御を行うためのプログラムが記録されたＲＯＭと、入出力手段とを備える。フラッシュメモリ１６はデジタルカメラ１に内蔵されるほか、デジタルカメラ１に着脱自在なメモリカードであってもよく、その両方を備えていてもよい。

【００１２】

使用者は、デジタルカメラ１に設けられる入力キーへの入力により、デジタルカメラにより撮影を行う撮影モード、すでに撮影した画像を表示する再生モード、デジタルカメラの作動について種々の設定を行う設定モードなどを切り替えることができる。

【００１３】

本実施例のデジタルカメラ１は、外部記録媒体２１（例えば、磁気ディスクやＣＤ－ＲＯＭ）に記録されたプログラムを、パーソナルコンピュータ２０のような外部の処理装置からデジタルカメラ１にインターフェイス１７を介して送信し、プログラムをデジタルカメラ１のフラッシュメモリ１６に導入（インストール

）することができる。プログラムを導入するためのプログラムもまた、外部記録媒体２１に記録され、パーソナルコンピュータ２０によって実行されることにより、プログラムのインストールが行われる。

【００１４】

フラッシュメモリ１６および外部記録媒体２１は、格納されるデータやプログラムをファイルとして格納し、ファイルの格納位置や属性を登録するファイルアロケーションテーブルによって各ファイルを管理するように構成されている。ファイルアロケーションテーブルに登録されるファイルの属性は、実行されるプログラムに対して各ファイルを識別させるためのものであって、その属性には、いずれのプログラムからも識別可能となる通常属性と、設定したプログラムのみが識別可能となる隠し属性とがある。

【００１５】

デジタルカメラ１にインストールされたプログラムは、デジタルカメラ１の制御部１１により実行することが可能である。デジタルカメラ１に着脱自在なメモリカード内にプログラムを記録し、デジタルカメラ１に内蔵されたフラッシュメモリ１６にプログラムを送信することにより、インストールしてもよい。プログラムのインストールは、デジタルカメラ１を購入後に所有者が自分で行ってもよく、また、プログラムがインストールされた状態で販売してもよい。

【００１６】

本実施例では、画像データに画像の改竄を検出するためのデータとして、画像データから生成した特徴データを電子透かしの方式で画像データに埋め込む手順を含むプログラム（以下透かしプログラム）をデジタルカメラにインストールする。透かしプログラムがインストールされると、デジタルカメラ１で撮影が行われた時には、通常の画像記録を行うプログラムに代わって、上記の透かしプログラムが実行され、画像データがフラッシュメモリ１６に記録される。撮影したときに通常の記録を行うか、透かしプログラムを実行させるかを、設定モードで選択できるようにしてもよい。

【００１７】

透かしプログラムと同時に、画像改竄検出データを暗号化するのに必要な秘密

鍵データが外部記録媒体２１からデジタルカメラ１に内蔵されたフラッシュメモリ１６に転送される。透かしプログラムをインストールするためのプログラムを複数用意し、例えば１２８ビットの秘密鍵データがインストールされるプログラム、２５６ビットの秘密鍵データがインストールされるプログラム、５１２ビットの秘密鍵データがインストールされるプログラムの３種類の中から実行するプログラムを使用者が選択することができる。これにより、簡易な暗号化でよい場合と、特に信頼性が必要な場合とで暗号化のレベルを使い分けることができる。

【００１８】

秘密鍵データは、外部記録媒体２１およびデジタルカメラ１に内蔵されたフラッシュメモリ１６の中で隠し属性のファイルとして扱われる。そのため、秘密鍵データの内容が容易に読み出されることがない。また、外部記録媒体２１に秘密鍵データを暗号化して記録し、デジタルカメラ１にその暗号を復号する手段を設け、暗号が復号された秘密鍵データをフラッシュメモリ１６に書き込むことにより、秘密鍵データをより安全に扱うことが可能である。

【００１９】

また、デジタルカメラ１に、すでに透かしプログラムがインストールされている場合には、秘密鍵データのみを外部記録媒体２１からデジタルカメラ１に導入してもよい。これにより、秘密鍵データの内容が他人に知られてしまったことが明らかになった場合などに、別の秘密鍵を転送して書き換えることにより安全に使用することができる。

【００２０】

図１は、透かしプログラムをインストールしたデジタルカメラ１により撮影が行われる行程を示すフローチャートである。ユーザーがデジタルカメラ１のシャッターを押すと、ステップＳ１０１で、集光レンズ１２により集光された光がＣＣＤ１３に入力され、電気信号に変換される。集光レンズ１２の絞りやシャッタースピード、すなわちＣＣＤ１３の蓄積時間は制御部１１によって自動的に、またはユーザーの指示によって制御される。ＣＣＤ１３として、例えばＲ（Red）、Ｇ（Green）、Ｂ（Blue）の原色フィルタを有する複数の画素がマトリックス状に配置されたＣＣＤ１３を用いることにより、カラー画像を撮影することがで

きる。Ｃ（Cyan）、Ｍ（Magenta）、Ｙ（Yellow）、Ｇ（Green）の補色フィルタを有するＣＣＤを用いる場合もある。

【００２１】

ステップＳ１０２では、ＣＣＤ１３から出力された電気信号がＡ／Ｄ変換部１４によりデジタル信号に変換され、ステップＳ１０３ではＡ／Ｄ変換部１４から出力されたデジタルデータが高速化のためＤＭＡ（Direct Memory Access）により制御部１１を介さずに直接ＲＡＭ１５のアドレスを指定して記録される。ＲＡＭ１５としてはセルフリフレッシュ機能をもつＤＲＡＭを用いることができる。

【００２２】

ステップＳ１０４では、ＲＡＭ１５に記録されたデータについて、ホワイトバランスの調整、補間処理、色補正などの各種の画像補正が行われる。ここで、画像の拡大・縮小など、その他の画像処理を行ってもよい。

【００２３】

ステップＳ１０５～Ｓ１１０では、画像記録媒体への記録枚数を多くするためにステップＳ１０４で補正されたデータをＪＰＥＧ（Joint Photographic Experts Group）などの方式により圧縮し、容量の小さな画像データを生成する。ＪＰＥＧ圧縮は、制御部１１によってソフトウェア的に行うほか、高速化のために専用の回路を用いることができる。

【００２４】

以下にＪＰＥＧ圧縮の手順を説明する。ステップＳ１０５では、まず画像データを８×８画素を１単位とした複数のブロックに分割する。例えば、６４０×４８０画素の画像データであれば、８０×６０＝４８００ブロックに分割され、ブロック単位に処理が行われる。

【００２５】

次に、Ｂ１～Ｂ４８０の各ブロックごとに画素同士の濃度の相対関係（空間周波数）を調べ、ＤＣＴ（拡散コサイン変換）方式により、各ブロックを低周波数項のＤＣＴ０から高周波数項のＤＣＴ６３に分ける。ＤＣＴ０～ＤＣＴ６３はそれぞれ８ビットの値である。図３には、高周波数項のＤＣＴ６３を１６進数で示している。そして、所定の量子化テーブルを用いて量子化することにより高周波

数項の多くが０となるようにし、後の行程でハフマン符号化したときに圧縮率が高くなるようにする。

【００２６】

ステップＳ１０６では、後の行程で特徴データを埋め込む位置を決定するために、ブロック化されＤＣＴ変換された画像データの先頭のブロックから順に各ブロックで最も高周波側の成分であるＤＣＴ６３を調べる。そして、ＤＣＴ６３の値が、０および１以外のブロックを埋め込みブロックとして記憶する。図３に示す例では、Ｂ３、Ｂ４、Ｂ５及びＢ６が①、②、③および④の埋め込みブロックとして選択され記憶される。本実施例では１２８ビットのハッシュ値を用いるために、１２８のブロックを選択する。埋め込みブロックが１２８ブロックに満たない場合は、足りない埋め込みブロック数と未調査のブロックが一致した時点で、残りのブロックを全て埋め込みブロックとする。そして埋め込みブロックのＤＣＴ６３の最下位ビットを全て０に置き換える。これにより、例えばブロックＢ４のＤＣＴ６３はＦＦからＦＥに書き換えられるが、高い周波数における小さな変動は、肉眼ではほとんど判断することができないため、画像の歪みは最小限となる。

【００２７】

ステップＳ１０７では、ステップＳ１０６で部分的に書き換えられた画像データに基づいて、制御部１１により特徴データを生成する。特徴データとしては、例えば種々の一方向ハッシュ関数により算出されるハッシュ値を用いることができる。また、ハッシュ値の他に、チェックサム、ＣＲＣ方式等、データがオリジナルから変更されているか否かを検出することができる公知の方法を本発明に適用することもできる。これらの方法を用いることにより、各々の画像データに対して異なる特徴データを割り当てることができ、また、特徴データから元の画像データを再現することはほとんど不可能となる。本実施例では、特徴データとして１２８ビットのハッシュ値を算出する。例えば、ＭＤ５、ＳＨＡあるいはＲＩＰＥＭＤハッシュ関数を用いることができる。

【００２８】

ステップＳ１０８では、ハッシュ値などの特徴データが解析されたり容易に書

き換えられたりしないように、制御部１１により暗号化して暗号化データとする。暗号化の方法としては、公開鍵と秘密鍵を用いるＲＡＳ方式など、公知の方法を用いることができる。秘密鍵で暗号化した暗号化データは、秘密鍵と対になった公開鍵を用いて復号化することができる。秘密鍵はデジタルカメラ１内に隠し属性のファイルとして記録されている。秘密鍵は、他人に知られてはならず、また、本実施例ではユーザーが秘密鍵を知る必要はない。一般に、公開鍵から、それに対応する秘密鍵を求めることは非常に困難である。これにより、画像データが同一の特徴データを得られる別の画像データに変更されることや、画像データの変更に合わせて特徴データが書き換えられるのを防ぐことができる。

【００２９】

ステップＳ１０９では、ハッシュ値を暗号化した暗号化データを、選択された埋め込みブロックのＤＣＴ６３の最下位ビットに１ビットずつ書き込むことにより、画像の劣化を最小限にして特徴データを画像データの中に埋め込む。なお、ＪＰＥＧ形式の画像データは、カラー画像の場合は、Ｙ（輝度）、Ｕ、Ｖ（色相）の成分を有するが、暗号化された特徴データはＹ成分に埋め込まれる。

【００３０】

ステップＳ１１０では、暗号化データが埋め込まれたデータをハフマン符号化することにより、データの圧縮を行う。ハフマン符号化では、データの可逆性は満足されており、処理の前後でデータの欠損はない。Ｓ１０５での量子化テーブルによる量子化の度合いを変えることによって圧縮率を変更することができる。

【００３１】

ステップＳ１１１では、Ｓ１１０で圧縮された画像データをＪＰＥＧファイル３０として画像記録媒体としてのフラッシュメモリ１６に記録する。フラッシュメモリ１６は通電しなくても記録内容を保存することのできる書換え可能な記録媒体であり、デジタルカメラ１に内蔵されるか、あるいは着脱自在にデジタルカメラ１に取り付けられている。一般にＪＰＥＧファイル３０は図４に示すようにデータ長、圧縮率等の情報を含むヘッダ部３１と、画像データ部３２とから構成される。デジタルカメラ１によって記録されるＪＰＥＧファイル３０の場合は、撮影日や撮影条件等の情報もヘッダ部３１に記録されることがある。本実施例で

は、暗号化に用いた秘密鍵に対応する公開鍵３３をヘッダ部３１に更に加えて記録している。

【００３２】

設定モードで透かしプログラムを実行しないように設定されている場合は、通常のＪＰＥＧ圧縮と同様の手順により、ステップＳ１０５でＤＣＴ変換され量子化されたデータはステップＳ１１０でハフマン符号化により圧縮される。

【００３３】

上記の例では、ＪＰＥＧ圧縮の途中の行程で特徴データを埋め込んだが、特徴データの埋め込みを行わずにハフマン符号化まで行う通常のＪＰＥＧ圧縮を行った後に、部分的に画像データを復号し、ステップＳ１０６～Ｓ１０９と同様の行程により特徴データを埋め込み、再度ハフマン符号化してもよい。

【００３４】

上記のようなデジタルカメラ１と、デジタルカメラ１から出力された画像データを入力する手段を備えるパーソナルコンピュータ２０等のコンピュータと、デジタルカメラ１によって記録された画像データが変更されたか否かを判定するためにパーソナルコンピュータ２０等にインストールされた検出プログラムとによって画像改竄検出システムが構成される。

【００３５】

本実施例の画像改竄検出システムにより画像の改竄を検出する行程を図５に示すフローチャートを用いて説明する。

ステップＳ２０１では、検出プログラムにより、パーソナルコンピュータ２０にデジタルカメラから画像データが読み込まれる。パーソナルコンピュータ２０に画像データを読み込む手段としては、シリアルケーブル１８等を介してデジタルカメラ１のインターフェイス１７と接続してフラッシュメモリ１６内のＪＰＥＧファイルをパーソナルコンピュータ２０に転送する方法や、フラッシュメモリ１６が着脱自在でパーソナルコンピュータ２０と互換性のある形式でフォーマットされている場合には、アダプタを介してフラッシュメモリ１６に記録されたＪＰＥＧファイル３０をパーソナルコンピュータ２０で直接読取ることも可能である。

【００３６】

ステップＳ２０２では、画像データを復号化し、上記のステップＳ１０６で特徴データを埋め込むブロックを選択したときと同様の手順で、特徴データが埋め込まれているべきブロックを選択し、１２８ビットの暗号化データを抽出する。

【００３７】

ステップＳ２０３では、暗号化データが埋め込まれていたビットに全て０を書き込み、暗号化データが埋め込まれる前の元画像データを生成する。

ステップＳ２０４では、ステップＳ１０７と同様の手順で、１２８ビットのハッシュ値を算出する。

【００３８】

ステップＳ２０５では、ステップＳ２０２で抽出した暗号化データを、ＪＰＥＧファイルのヘッダに書き込まれた公開鍵を用いて、秘密鍵によって暗号化されたことを確認すると同時に暗号を復号化する。それにより、暗号化前のハッシュ値を求める。

【００３９】

ステップＳ２０６では、ステップＳ２０４で算出されたハッシュ値とステップＳ２０５で算出されたハッシュ値を比較し、一致していれば画像データは本実施例のデジタルカメラ１により撮影された後に改竄されていないものであると判定し、一致しなければ画像データは撮影時から改竄された可能性があると判定する。また、ステップＳ２０５で、暗号化データが公開鍵で復号化できない場合にも、その画像データは本発明実施例のデジタルカメラ１で撮影されたものではないか、撮影後に変更されたものとみなされる。

【００４０】

したがって、本発明実施例の画像改竄検出システムを使用する場合、写真の提出者は、デジタルカメラ１から出力して変更を加えていない画像データを含むファイル（本実施例ではＪＰＥＧファイル３０）をフロッピー等の記録媒体に記録したもの、あるいは着脱可能な記録媒体であるフラッシュメモリ１６をデジタルカメラ１から取り外したものを、印刷した写真と共に、あるいは相手の求めに応じて提出する。受け取り側は、パーソナルコンピュータ２０にインストールされ

た検出プログラムを用いて受け取ったファイルを読み込んで調べることにより、そのファイルの画像データがデジタルカメラ１から出力された時点から変更されていないということを確認することができる。

【００４１】

また、検出プログラムにＪＰＥＧファイル３０等の画像データの画像を表示する機能をもたせることにより、印刷された写真と表示された画像が同一であることを確認することができる。

【００４２】

また、本実施例では、ＪＰＥＧファイル３０のヘッダ部３１に付加された公開鍵を用いて、暗号を復号化したが、検出プログラムが複数の秘密鍵に対応する複数の公開鍵を含むリストを記憶してその中から１つの公開鍵を選択して暗号を復号することもできる。これにより、そのため、本発明による特徴データの生成方法、暗号化方法、画像データへの埋め込み方などのアルゴリズムを知る者が、自分で公開鍵と秘密鍵の組み合わせを作成し、本発明と同様の処理をパソコンなどを用いて行い画像データを作成した場合でも、その画像データに付加された公開鍵が、あらかじめ用意された公開鍵のリストに含まれないものであれば、その画像データは改竄された可能性があると判断することができる。なお、画像改竄検出システムに記録される複数の公開鍵が知られたとしても、公開鍵から秘密鍵を算出することはほぼ不可能であるため、秘密鍵が他人に知られる恐れはない。

【００４３】

上記の実施例では、ＪＰＥＧ圧縮したものを画像データとして画像記録媒体に記録したが、本発明は他の圧縮方法で圧縮したものや、無圧縮のデータを画像データとして記録したものにも適用できる。また、本実施例では、特徴データを暗号化してＪＰＥＧファイルの画像データ部分の中に埋め込んで記録したが、本発明としてはヘッダ部に書き込むなど、特徴データは画像データのどの位置にあってもよい。

【図面の簡単な説明】

【図１】

本発明の実施例におけるデジタルカメラにより画像を記録する手順を示すフロ

ーチャートである。

【図２】

本発明の実施例によるデジタルカメラを示すブロック図である。

【図３】

本発明の実施例による画像データの特徴データを算出する方法を説明するための模式図である。

【図４】

本発明の実施例によるＪＰＥＧファイルの構造を説明するための模式図である。

【図５】

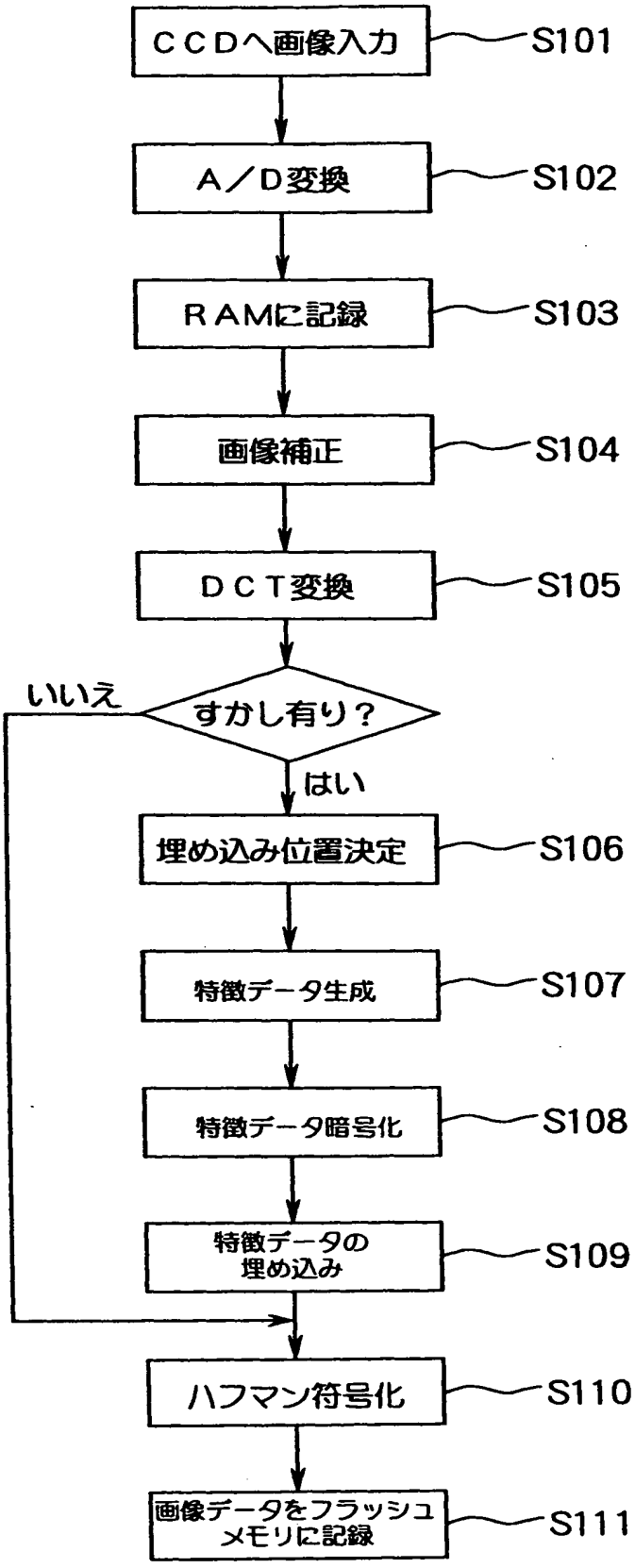
本発明の実施例により画像データの改竄を検出する手順を示すフローチャートである。

【符号の説明】

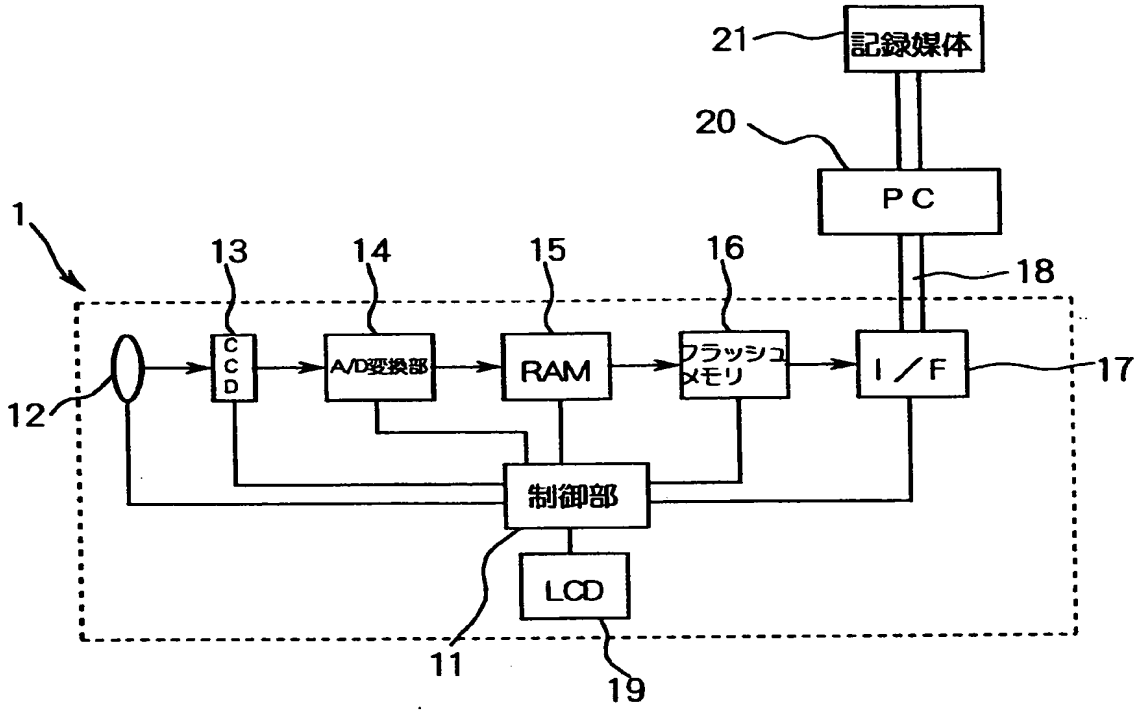
１　デジタルカメラ
１１　制御部
１２　集光レンズ
１３　ＣＣＤ（撮像部）
１４　Ａ／Ｄ変換部
１５　ＲＡＭ
１６　フラッシュメモリ
１７　インターフェイス
１８　接続ケーブル
１９　液晶表示部（ＬＣＤ）
２０　パーソナルコンピュータ
２１　外部記録媒体
３０　ＪＰＥＧファイル
３１　ヘッダ部
３２　画像データ
３３　公開鍵

【書類名】　　図面

【図１】


ＣＣＤへ画像入力
S101
Ａ／Ｄ変換
S102
ＲＡＭに記録
S103
画像補正
S104
ＤＣＴ変換
S105
いいえ
すかし有り？
はい
埋め込み位置決定
S106
特徴データ生成
S107
特徴データ暗号化
S108
特徴データの
埋め込み
S109
ハフマン符号化
S110
画像データをフラッシュ
メモリに記録
S111

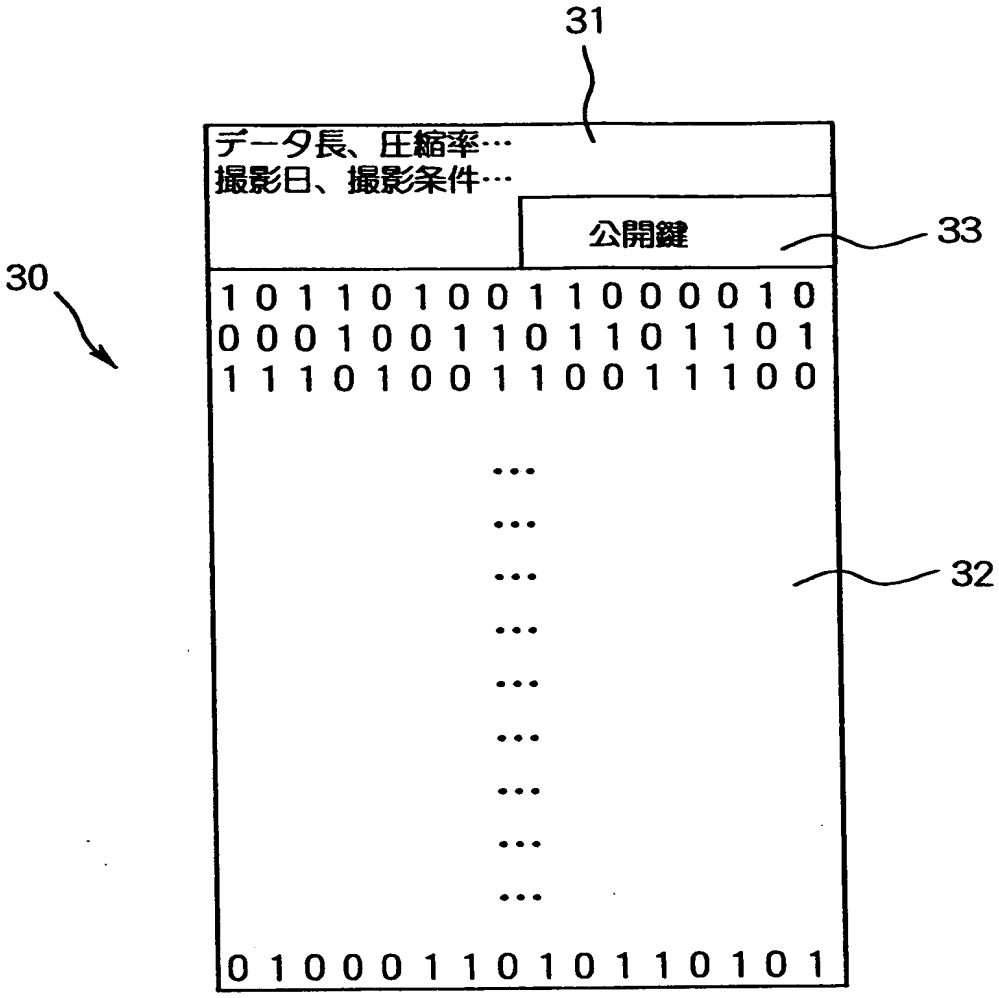
【図２】



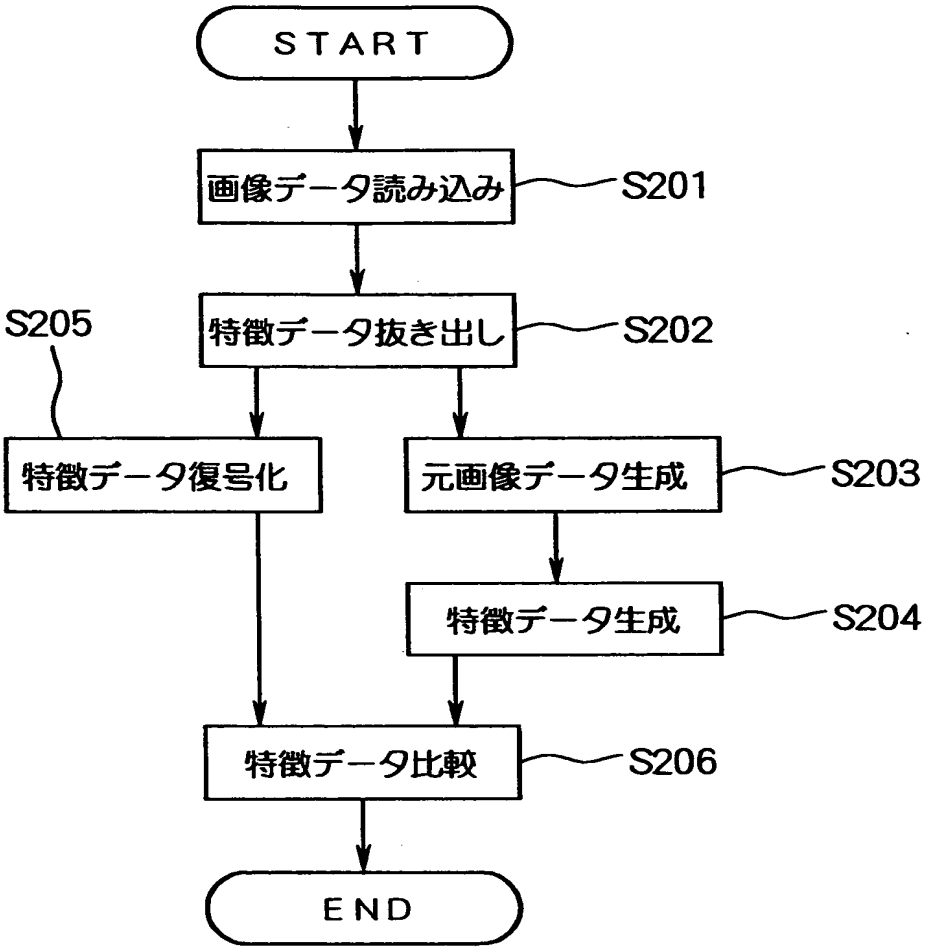

【図３】

| | | | |
|---|---|---|---|
| B1 ……00 | B2 ……01 | B3 ① ……02 | B4 ② ……FF |
| B5 ③ ……E5 | B6 ④ ……14 | B7 ……00 | B8 ……01 |
| | | | |

【図４】


31
データ長、圧縮率…
撮影日、撮影条件…
公開鍵
33
30
1 0 1 1 0 1 0 0 1 1 0 0 0 0 1 0
0 0 0 1 0 0 1 1 0 1 1 0 1 1 0 1
1 1 1 0 1 0 0 1 1 0 0 1 1 1 0 0
32
0 1 0 0 0 1 1 0 1 0 1 1 0 1 0 1

【図５】


START
画像データ読み込み
S201
特徴データ抜き出し
S202
S205
特徴データ復号化
元画像データ生成
S203
特徴データ生成
S204
特徴データ比較
S206
END

【書類名】　　要約書

【要約】

【課題】　撮影時の画像データから改竄されたか否かを確認することのできる画像データを出力するデジタルカメラを提供する。

【解決手段】　ステップＳ１０１ではＣＣＤから出力された電気信号をデジタル信号に変換する。ステップＳ１０３ではＡ／Ｄ変換器から出力されたデジタルデータをＲＡＭに記録する。ステップＳ１０４ではＲＡＭに記録されたデータについて各種の画像補正を行う。ステップＳ１０５～Ｓ１１０ではステップＳ１０４で補正されたデータをＪＰＥＧ方式により圧縮する。ステップＳ１０６で特徴データの埋め込み位置を決定し、ステップＳ１０７で画像データから特徴データを生成する。ステップＳ１０８では特徴データを暗号化して暗号化データとする。ステップＳ１０９では画像データの中に暗号化された特徴データを埋め込む。

【選択図】　　図１

# 出　願　人　履　歴　情　報

識別番号　　〔０００００２３６９〕

１．変更年月日　　１９９０年　８月２０日
［変更理由］　新規登録
住　所　　東京都新宿区西新宿２丁目４番１号
氏　名　　セイコーエプソン株式会社